Number Theory. Problem set III .

Due date: December, 26, 2017.

1. (a) Let $K \supset \mathbb{Q}$ be a finite extension, $O_K \subset K$ the maximal order, r_2 the number of complex (not real) embeddings $K \hookrightarrow \mathbb{C}$ up to complex conjugation, $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$. Prove that

$$Vol(K_{\mathbb{R}}/O_K) = 2^{-r_2}\sqrt{Disc(K/\mathbb{Q})}.$$

Here $Disc(K/\mathbb{Q})$ stands for the discriminant of the extension. (Note, the $\mathbb{R}$-algebra $K_{\mathbb{R}}$ is isomorphic to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and that the induced from $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ volume form does not depend on the choice of this isomorphism. Therefore the expression $Vol(K_{\mathbb{R}}/O_K)$ makes sense.)

(b) Prove that every finite extension $K \supset \mathbb{Q}$ of degree greater than 1 is ramified at least over one prime. [1] (Hint: Use the Minkowski Lemma and part (a).)

2. Let $p > 2$ be a prime number, μ_p a p-th primitive root of 1 in $\mathbb{C}$.

(a) Show $\mathbb{Z}[\mu_p] \subset \mathbb{Q}(\mu_p)$ is the maximal order and that the extension $\mathbb{Q}(\mu_p) \supset \mathbb{Q}$ is unramified except over prime p.

(b) For each $l \neq p$ compute the Frobenius element $F_l \in Gal(\mathbb{Q}(\mu_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p)^*$.

3. (a) Let $f(x)$ be a monic polynomial of degree n with integral coefficients which has no multiple complex roots, D the discriminant of $f(x)$, and let $K \supset \mathbb{Q}$ be the splitting field of $f(x)$. The Galois group $Gal(K/\mathbb{Q})$ acts on the set of roots of $f(x)$ and this action defines an embedding $Gal(K/\mathbb{Q}) \subset S_n$.

(a) Show that if p does not divide D then K is unramified over p.

(b) Assume that p does not divide D. Let $\overline{f}(x) = \overline{f}_1(x) \cdots \overline{f}_l(x)$ be the factorization of the reduction of $f(x)$ modulo p into a product of irreducible polynomials. Let d_i be the degree of $\overline{f}_i(x)$. Prove the cycle type of the Frobenius element F_p regarded as a conjugacy class in S_n is $(d_1, \cdots, d_l)$.

4. Let $f(x)$ be a polynomial with integral coefficients.

(a) Prove that there are infinitely many primes p such that the reduction of $f(x)$ modulo p splits into a product of linear factors.

(b) Assume that for all but finitely many primes p the reduction of $f(x)$ modulo p splits into a product of linear factors. Prove that $f(x)$ splits into a product of linear factors in $\mathbb{Q}[x]$.

Remark: The assertions from parts (a) and (b) follow readily from Chebotarev's density theorem and Problem 3. However, I invite you to give a direct proof using the following result from the lectures: for any finite extension $\mathbb{Q} \subset K$ the limit $(s-1)\zeta_K(s)$ as $s \to 1$ exists and does not equal to 0.)

(c) Assume that for all but finitely many primes p the reduction of $f(x)$ modulo p has a zero in $\mathbb{F}_p$. Prove that $f(x)$ is reducible.

(d) Prove, that the polynomial $f(x) = (x^2-3)(x^2-5)(x^2-15)$ has a zero in $\mathbb{F}_p$ for every prime p but does not have rational zeros.

---

[1] Using the language of algebraic geometry this assertion means that $spec\,\mathbb{Z}$ is simply connected.

5. (a) Let $1 \neq \epsilon \in \mathbb{C}^*$ be a n-th root of 1. Compute the sum

$$\sum_{n=1}^{\infty} \frac{\epsilon^n}{n}.$$

(b) Let $f : G = \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ be a function , $\hat{f} : \hat{G} \simeq \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ its Fourier transform. Assume that $\sum_{m \in \mathbb{Z}/n\mathbb{Z}} f(m) = 0$. Prove that the series

$$\sum_{n=1}^{\infty} \frac{f(n)}{n}$$

is convergent and find its sum.
(c) Compute

$$\sum_{n=1}^{\infty} \left(\frac{1}{4n} - \frac{1}{4n+1}\right).$$

6. Let p be a prime of the form $4k+3$, $K = \mathbb{Q}(\sqrt{-p})$, and $\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*$ Legendre symbol $\chi(m) = (m/p)$.
(a) Prove that

$$\zeta_K(s) = \zeta(s) L(s, \chi).$$

(b) Prove that if, in addition, $p \neq 3$, then

$$L(1, \chi) = -\frac{\pi}{p\sqrt{p}} \sum_{m=1}^{p-1} \chi(m) m.$$

(When solving this problem you may use the following fact. Let $\epsilon = cos\frac{2\pi}{p} + isin\frac{2\pi}{p}$ and

$$G = \sum_{m=1}^{p-1} \chi(m) \epsilon^m$$

be the Gauss sum. Gauss proved that $G = i\sqrt{p}$, where $\sqrt{p}$ is the positive root. (We computed G up to sign on the 2-nd lecture.)
(c) Let h_K be the class number of K, V the number of quadratic residues modulo p on the interval $(0, p/2)$, N the number of nonresidues on the same interval. Prove that if $p \equiv 7\,(mod\,8)$, then

$$h_K = V - N,$$

and if $p \equiv 3\,(mod\,8)$ and $p \neq 3$, then

$$h_K = \frac{1}{3}(V - N).$$